デスクトップ マネジメントについて
Business Desktop

製品番号：361202-291

2004年5月

このガイドでは、一部のモデルにプリインストールされているセキュリティ機能とインテリジェント マネジメント機能の概念および使用手順について説明します。

本書の内容は、将来予告なしに変更されることがあります。

MicrosoftおよびWindowsは、米国Microsoft Corporationの米国およびその他の国における登録商標です。

その他、本書に掲載されている会社名、製品名はそれぞれ各社の商標または登録商標です。

HP製品およびサービスに対する保証は、当該製品およびサービスに付属の保証規定に明示的に記載されているものに限られます。**本書のいかなる内容も、当該保証に新たに保証を追加するものではありません。**本書の内容につきましては万全を期しておりますが、本書の技術的あるいは校正上の誤り、省略に対しては、責任を負いかねますのでご了承ください。

本書には、著作権によって保護された所有権に関する情報が掲載されています。本書のいかなる部分も、Hewlett-Packard Companyの書面による承諾なしに複写、複製、あるいは他言語へ翻訳することはできません。

本製品は、日本国内で使用するための仕様になっており、日本国外で使用される場合は、仕様の変更を必要とすることがあります。

本書に記載されている製品情報は、日本国内で販売されていないものも含まれている場合があります。

以下の記号は、本文中で安全上重要な注意事項を示します。

警告：その指示に従わないと、人体への傷害や生命の危険を引き起こす恐れがあるという警告事項を表します。

注意：その指示に従わないと、装置の損傷やデータの損失を引き起こす恐れがあるという注意事項を表します。

デスクトップ マネジメントについて
Business Desktop
初版 2004年5月
製品番号：361202-291

日本ヒューレット・パッカード株式会社

目次

デスクトップ マネジメント

索引

デスクトップ マネジメント

HPのインテリジェント マネジメント機能は、ネットワーク環境にあるデスクトップ、ワークステーション、およびノートブック コンピュータの管理と制御の分野で、標準のソリューションを提供しています。HPはデスクトップ マネジメントのパイオニアとして1995年に、デスクトップを完全に管理できる業界初のパーソナル コンピュータを世に送り出しました。HPはマネジメント機能の特許を取得しています。以来、デスクトップ、ワークステーション、およびノートブック コンピュータの効果的な導入、設定、および管理に必要な標準化とインフラストラクチャの開発において業界全体の取り組みをリードしてきました。HPは、業界トップ クラスの管理ソフトウェア ソリューション提供企業との提携関係により、これらの企業の製品とインテリジェント マネジメント機能の互換性を確保しています。インテリジェント マネジメント機能は、ライフサイクル ソリューションを提供する幅広い取り組みの中でも重要な位置を占めるもので、デスクトップ コンピュータのライフサイクルの4つの側面である計画、導入、管理、移行でユーザをサポートします。

デスクトップ マネジメントの主要な機能と特長は、次のとおりです。

- 出荷時設定の変更
- リモート システム インストール
- ソフトウェア アップデートおよびマネジメント機能
- ROMフラッシュ
- 資産情報管理機能およびセキュリティ機能
- 障害通知および復旧機能

このガイドで説明される機能のサポートについては、機種またはソフトウェアのバージョンにより異なることがあります。

出荷時設定の変更

お使いのコンピュータには、システム ソフトウェア イメージがプリインストールされています。ソフトウェアの設定手順を簡単に済ませると、すぐにコンピュータを使用できます。

プリインストールされたソフトウェア イメージの代わりにカスタマイズされたシステム ソフトウェアおよびアプリケーション ソフトウェアを使うこともできます。カスタマイズされたソフトウェア イメージを展開するには、いくつかの方法があります。

- プリインストールされたソフトウェア イメージを展開した後、追加するアプリケーションをインストールする。
- Altiris Deployment Solutionsなどのソフトウェアの導入用ツールを使用して、プリインストール ソフトウェアの代わりにカスタマイズされたソフトウェア イメージを使用する。
- ディスク複製手順を使用して、ハードディスク ドライブの内容を別のハードディスクにコピーする。

最適なコンピュータ環境の構築方法は、お使いの情報技術環境や作業内容によって異なります。HPライフサイクル ソリューションに関する弊社のホームページ（http://whp-sp-orig.extweb.hp.com/country/us/en/solutions.html、英語サイト）には、お使いの環境に適したコンピュータの導入方法を選択する際に役立つ情報が掲載されています。

Restore Plus! CD、ROMからのセットアップ、およびACPIハードウェアにより、システム ソフトウェアのリストア、コンフィギュレーション マネジメント機能、トラブルシューティング、および省電力機能を利用することができます。

リモート システム インストール

Preboot Execution Environment（PXE）を起動すれば、リモート システム インストールを使用してネットワーク サーバからソフトウェアやコンフィギュレーション情報（コンピュータの設定情報）を取り出して、コンピュータを起動したりセットアップしたりすることができます。リモート システム インストールの機能は、通常、システム セットアップやコンフィギュレーションのためのツールとして使用しますが、次のような場合にも使用できます。

- ハードディスク ドライブをフォーマットするとき
- 1台以上の新しいコンピュータにソフトウェア イメージを導入するとき
- フラッシュ ROMを使用してシステムBIOSをリモートでアップデートするとき（7ページの「リモートROMフラッシュ機能」を参照）
- システムBIOSを設定するとき

リモート システム インストールを起動するには、起動時に表示されるHPロゴの画面の右下隅に[F12 = Network Service Boot]と表示されたら、すぐに**[F12]**キーを押します。画面のメッセージに従って、リモート システム インストールを起動します。デフォルトの起動順序はBIOSのコンフィギュレーションの設定ですが、常にPXEを起動するように変更できます。

HPとAltiris社の提携により、企業におけるコンピュータの導入と管理を短時間で容易に実行できるツールが開発されました。このツールを使用すると、TCO（維持管理費）が大幅に削減されます。HPのコンピュータが、企業環境内で最も管理しやすいクライアント マシンになります。

ソフトウェアのアップデートと管理

HPでは、デスクトップ コンピュータおよびワークステーションのソフトウェアを管理し、アップデートするためのツール（HP Client Manager Software、Altiris Client Management Solutions、System Software Manager、Proactive Change Notification（製品変更通知）、およびSubscriber's Choice）を提供しています。

HP Client Manager Software

HP Client Manager Software（HP CMS）は、以下の機能により、クライアントコンピュータのハードウェアの管理に役立ちます。

- 資産管理用のハードウェア インベントリの詳細表示
- コンピュータの状態検査の監視および診断
- ハードウェア環境の変化についての事前通知
- マシン温度についての警告、メモリ異常の警告など、企業活動における重大な状況についての、Webサイトを利用した報告
- システム ソフトウェア（デバイス ドライバやROM BIOSなど）のリモート アップデート
- 起動順序のリモートからの変更

HP Client Managerについて詳しくは、http://h18000.www1.hp.com/im/client_mgr.html（英語サイト）を参照してください。

Altiris Client Management Solutions

HPはAltiris社と提携して、HPクライアントPCの所有によるコストを削減する、強力に統合された包括的なシステム管理ソリューションを提供しています。Altiris Client Management Solutionsは、HP Client Manager Softwareを基礎としており、次の機能があります。

- 資産管理
  - ソフトウェア ライセンスの準拠
  - コンピュータの管理および報告
  - リース契約および固定資産の管理

- 展開と移行
  - Microsoft® Windows® XP ProfessionalまたはHome Editionへの移行
  - システムの展開
  - 個人設定の移行
- ヘルプデスクと問題解決
  - ヘルプデスク チケットの管理
  - リモートでのトラブルシューティング
  - リモートでの問題解決
  - クライアントでの問題修復
- ソフトウェアおよび操作の管理
  - デスクトップ マネジメントの実行
  - HPシステム ソフトウェアの展開
  - アプリケーションの自己修復

Altiris Solutionsの詳細情報および30日間試用版のダウンロード方法については、http://h18000.www1.hp.com/im/prodinfo.html#deploy（英語サイト）を参照してください。

一部のデスクトップおよびノートブック コンピュータには、工場出荷時にロードされたイメージの1つとしてAltirisマネジメント エージェントが含まれています。このエージェントによりAltiris Development Solutionsとの通信が可能になります。Altiris Development Solutionsを使用すると、簡単なウィザードに従って、新しいハードウェアの展開や新しいオペレーティング システムへの個人設定の移行を完了することができます。Altiris Solutions ソフトウェアには、使いやすいソフトウェア配布機能も含まれています。System Software ManagerまたはHP Client Manager Softwareと組み合わせて使用すると、管理者はROM BIOSとデバイス ドライバのソフトウェアを中央管理コンソールからアップデートすることもできます。

詳しくは、HPのWebサイト、http://h18000.www1.hp.com/im/index.html（英語版）を参照してください。

System Software Manager

System Software Manager（SSM）は、複数のシステムにおいてシステム レベルのソフトウェアを同時にアップデートできるユーティリティです。SSMは、コンピュータのクライアント システムで使用すると、ハードウェアおよびソフトウェアのバージョンを検出し、ファイル格納ディレクトリと呼ばれる中央のリポジトリから適切なソフトウェアをアップデートします。SSMでサポートされるドライバのバージョンは、ドライバのダウンロード サイトおよびサポート ソフトウェアCDに、独自のアイコンで示されています。ユーティリティのダウンロードまたはSSMについて詳しくは、http://www.hp.com/go/ssm（英語サイト）を参照してください。

Proactive Change Notification

Proactive Change Notificationプログラムは、Subscriber's ChoiceのWebサイトを利用して、以下のことを事前にかつ自動的に行います。

- ほとんどの企業向けHP製コンピュータおよびサーバでハードウェアおよびソフトウェアの変更があった場合に、最も早くて60日前に電子メールでProactive Change Notification（PCN）を通知する
- ほとんどの企業向けHP製コンピュータおよびサーバについてのCustomer Bulletins、Customer Advisories、Customer Notes、Security Bulletins、およびDriver alertsを含んだ電子メールを送信する

特定のIT環境に該当する情報のみを受け取るようにするため、ユーザ専用のプロファイルを作成します。Proactive Change Notificationプログラムの詳細およびカスタム プロファイルの作成方法については、http://h30046.www3.hp.com/subhub.php?jumpid=go/pcn（英語サイト）を参照してください。

Subscriber’s Choice

Subscriber’s ChoiceはHPのクライアントベースのサービスです。ユーザのプロファイルを基に、製品の使用のヒント、特集記事、およびドライバやサポートに関する警告や通知を提供します。Subscriber’s Choice Driver and Support Alerts/Notificationsでは、購読するようプロファイルに設定した情報が閲覧および入手可能になると、電子メールで通知します。Subscriber’s Choiceの詳細およびカスタム プロファイルの作成については、http://h30046.www3.hp.com/subhub.php（英語サイト）を参照してください。

ROMフラッシュ機能

お使いのコンピュータでは、オペレーティング システムとの情報のやりとりなどを行う基本入出力システム（BIOS）がプログラム可能なフラッシュROMに記憶されているので、必要に応じて簡単にアップグレードすることができます。ROMのアップグレードにはRomPaqディスケットが必要です。RomPaqディスケットは、インターネットのHPホームページからダウンロードできます。ROMのアップグレード手順については、RomPaqディスケットに付属の説明を参照してください。

注意：コンピュータにセットアップ パスワードを設定しておけば、システムROMの内容が不用意に変更されるのを防ぐことができます。コンピュータにセットアップ パスワードが設定されていないと、ROMへの書き込みが禁止されていないので、不用意にROMの内容が変更されてしまう危険があります。

システムROMのバージョンがお使いのコンピュータのモデルやオペレーティング システムに合っていないと、コンピュータが正しく動作しないことがあります。

System Software Managerを使用すると、システム管理者が、複数のコンピュータに同時にセットアップ パスワードを設定することができます。

詳しくは、http://www.hp.com/go/ssm（英語サイト）を参照してください。

リモートROMフラッシュ機能

リモートROMフラッシュ機能を利用すれば、システム管理者は、ネットワーク管理端末からリモートでコンピュータのROMを安全に書き換えることができます。複数のHPのコンピュータに対してこのような作業をリモートで行うことができるので、ネットワーク上のコンピュータのROMを適切にアップグレードし、少ない費用で管理することができます。

リモートROMフラッシュを使用するには、リモート ウェイク アップ機能を使って、お使いのコンピュータの電源を入れておくか、再起動しておく必要があります。

リモートROMフラッシュについて詳しくは、http://h18000.www1.hp.com/im/prodinfo.html（英語サイト）でHP Client Manager SoftwareまたはSystem Software Managerについての説明を参照してください。

HPQFlash

HPQFlashユーティリティは、Windowsオペレーティング システムで個別のコンピュータ上でシステムROMのアップデートや復元を行う場合に使用します。

HPQFlashについて詳しくは、http://www.hp.com/support/files（英語サイト）で画面の指示に従ってコンピュータ名を入力してください。

ブート ブロックROM

ブート ブロックROMが装備されているので、システムROMのアップグレード中に電源の障害が発生するなどしてROMの書き換えに失敗した場合も、システムROMを復旧またはアップグレードすることができます。ブート ブロックはROMフラッシュの際にも更新されない領域に収められており、コンピュータの電源が入れられるたびにシステムROMフラッシュをチェックし、以下のどれかの方法でコンピュータを起動します。

- システム ROM が有効な場合は、コンピュータは通常の方法で起動します。
- システムROMが有効でない場合は、システムROMの復旧作業を実行できるように、RomPaqディスケットからのコンピュータの起動を、ブート ブロックROMがサポートします。

一部のモデルでは、RomPaqCDから復旧することもできます。ISO RomPaqのイメージは、一部のモデルからダウンロード可能なRom SoftPaqに含まれています。

ブート ブロックROMによりシステムROMが有効でないことが検出されると、システム電源ランプが8回赤く点滅し（1秒間に1回点滅した後に2秒間休止）、同時にビープ音が8回鳴ります。ブート ブロックのリカバリ モードのメッセージが、画面に表示されます（一部のモデルのみ）。

ブート ブロックのリカバリ モードになったら、以下のように操作して、システムROMを復旧（アップグレード）してください。

1. ディスケット ドライブやCDドライブにディスケットまたはCDが入っている場合は取り出し、コンピュータの電源を切ります。
2. RomPaqディスケットをディスケット ドライブに挿入します。または、お使いのコンピュータで使用できる場合は、RomPaq CDをCDドライブに挿入します。
3. コンピュータの電源を入れます。

   RomPaqディスケットまたはRomPaq CDが認識されない場合、RomPaqディスケットを挿入してコンピュータを再起動するように指示されます。

   セットアップ パスワードが設定されている場合、Caps Lockランプが点灯し、パスワード入力を求められます。
4. セットアップ パスワードを入力します。

   RomPaqディスケットからの再起動が正しく行われ、システムROMの復旧またはアップグレードが正常に完了すると、キーボード上の3つのランプが点灯し、ビープ音が鳴ります。
5. ディスケットまたはCDを取り出して電源を切ります。
6. 電源を入れなおして、コンピュータを起動します。

次の表に、ブート ブロックROMによるさまざまなキーボード ランプの状態（コンピュータにPS/2キーボードが接続されている場合）を示します。また、各ランプの状態の意味およびランプの状態に応じて行う操作も示します。

ブート ブロックROMによるキーボード ランプの状態

ブート ブロック モード	ランプの色	ランプの状態	意味
Num Lock	緑色	オン	RomPaqディスケットまたはRomPaq CDが挿入されていないか、壊れているか、またはドライブが正常に動作していない
Caps Lock	緑色	オン	パスワードを入力してください
Num、Caps、Scroll Lock	緑色	Num Lock、Caps Lock、Scroll Lockの順に1個ずつ点滅	キーボードがネットワーク モードでロックされた
Num、Caps、Scroll Lock	緑色	オン	ブート ブロックROMフラッシュが完了した。コンピュータの電源を入れなおして、コンピュータを再起動してください

診断ランプは、USBキーボードでは点滅しません。

リプリケート セットアップ機能

以下のリプリケート セットアップ機能を使用すれば、管理者がコンピュータの設定情報（コンフィギュレーション情報）を他の同じモデルのコンピュータに簡単にコピーすることができます。この機能によって、複数のコンピュータに同じ設定を行う時間を短縮することができます。

これらの手順を行うには、ディスケット ドライブ、またはHP USBメモリなどのサポートされるUSBフラッシュ メディア デバイスが必要です。

1台のコンピュータへのコピー

注意:設定情報はモデルにより異なります。コピー元とコピー先のコンピュータが別のモデルの場合、ファイル システムが破損する恐れがあります。たとえば、dc7100 USからdx6100 STに設定情報をコピーしないでください。

1. 設定情報コピー元のコンピュータの電源を切ります。Windows を実行している場合は、**[スタート]→[シャットダウン]**（または**[終了オプション]**）**→[シャットダウン]**（または**[電源を切る]**）の順に選択します。
2. 設定情報保存用ディスケットまたはUSBフラッシュ メディア デバイスをここで挿入します。
3. コンピュータの電源を入れます。
4. コンピュータが起動したらすぐに**[F10]**キーを押したままにし、コンピュータ セットアップを実行します。必要であれば、**[Enter]**キーを押すと、タイトル画面をスキップできます。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータを再起動して、もう一度**[F10]**キーを押したままにしてください。

PS/2キーボードを使用している場合、[Keyboard Error]というメッセージが表示されることがありますが、無視してかまいません。

5. **[ファイル]**（File）**→[複製セットアップ]**（Replicated Setup）**→[リムーバブル メディアに保存]**（Save to Removable Media）の順に選択します。画面上のメッセージに従って操作し、設定情報ディスケットまたはUSBフラッシュ メディア デバイスを作成します。

6. 設定情報コピー先のコンピュータの電源を切り、設定情報ディスケットまたはUSBフラッシュ メディア デバイスを挿入します。
7. 設定情報コピー先のコンピュータの電源を入れます。
8. コンピュータが起動したらすぐに**[F10]**キーを押したままにし、コンピュータ セットアップを実行します。必要であれば、**[Enter]**キーを押すと、タイトル画面をスキップできます。
9. **[ファイル]→[複製セットアップ]→[システム構成の復元]**（Restore from Removable Media）の順に選択したあと、画面上のメッセージに従って操作します。
10. 設定が完了したら、コンピュータを再起動します。

複数のコンピュータへのコピー

注意：設定情報はモデルにより異なります。コピー元とコピー先のコンピュータが別のモデルの場合、ファイル システムが破損する恐れがあります。たとえば、dc7100 USからdx6100 STに設定情報をコピーしないでください。

この手順では設定情報ディスケットまたはUSBフラッシュ メディア デバイスの作成に少し時間がかかりますが、設定情報をコピー先のコンピュータにコピーする時間は大幅に短縮されます。

この手順を行うため、また起動可能USBフラッシュ メディア デバイスを作成するためには、起動可能ディスケットが必要です。起動可能ディスケットを作成するためにWindows XPを使用できない場合は、1台のコンピュータへのコピーの手順を実行してください（10ページの「1台のコンピュータへのコピー」を参照）。

1. 起動可能ディスケットまたはUSBフラッシュ メディア デバイスを作成します。13ページの「サポートされるUSBフラッシュ メディア デバイス」または16ページの「サポートされないUSBフラッシュ メディア デバイス」を参照してください。

注意：USBフラッシュ メディア デバイスから起動できないコンピュータもあります。コンピュータ セットアップ（F10）ユーティリティに表示されるデフォルトの起動順序で、USBデバイスがハードディスク ドライブより前にある場合、そのコンピュータはUSBフラッシュ メディア デバイスから起動できます。それ以外の場合は、起動可能ディスケットを使用してください。

2. 設定情報コピー元のコンピュータの電源を切ります。Windows を実行している場合は、**[スタート]**→**[シャットダウン]**（または**[終了オプション]**）→**[シャットダウン]**（または**[電源を切る]**）の順に選択します。
3. 設定情報保存用ディスケットまたはUSBフラッシュ メディア デバイスをここで挿入します。
4. コンピュータの電源を入れます。
5. コンピュータが起動したらすぐに**[F10]**キーを押したままにし、コンピュータ セットアップを実行します。必要であれば、**[Enter]**キーを押すと、タイトル画面をスキップできます。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータを再起動して、もう一度**[F10]**キーを押したままにしてください。

PS/2キーボードを使用している場合、[Keyboard Error]というメッセージが表示されることがありますが、無視してかまいません。

6. **[ファイル]**（File）→**[複製セットアップ]**（Replicated Setup）→**[リムーバブル メディアに保存]**（Save to Removable Media）の順に選択します。画面上のメッセージに従って操作し、設定情報ディスケットまたはUSBフラッシュ メディア デバイスを作成します。
7. BIOS Utility for Replicated Setup（リプリケート セットアップ用BIOSユーティリティ）をダウンロードして、この中に含まれるrepset.exeファイルを設定情報ディスケットまたはUSBフラッシュ メディア デバイスにコピーします。このユーティリティを入手するには、http://welcome.hp.com/support/filesでコンピュータの製品ファミリを入力します。
8. 設定情報ディスケットまたはUSBフラッシュ メディア デバイス上で、次のコマンドを含むautoexec.batファイルを作成します。

   repset.exe

9. 設定情報コピー先のコンピュータの電源を切ります。設定情報ディスケットまたはUSBフラッシュ メディア デバイスを挿入し、コンピュータの電源を入れます。設定ユーティリティが自動的に実行されます。
10. 設定が完了したら、コンピュータを再起動します。

起動可能デバイスの作成

サポートされるUSBフラッシュ メディア デバイス

HP USBメモリなどのサポートされるデバイスには、そのデバイスを簡単な手順で起動可能にするためのイメージがプリインストールされています。使用しているUSBフラッシュ メディア デバイスにこのイメージが存在しない場合は、後で説明する手順に従ってください（16ページの「サポートされないUSBフラッシュ メディア デバイス」を参照）。

注意：USBフラッシュ メディア デバイスから起動できないコンピュータもあります。コンピュータ セットアップ（F10）ユーティリティに表示されるデフォルトの起動順序で、USBデバイスがハードディスク ドライブより前にある場合、そのコンピュータはUSBフラッシュ メディア デバイスから起動できます。それ以外の場合は、起動可能ディスケットを使用してください。

起動可能なUSBフラッシュ メディア デバイスを作成するには、次のものが必要です。

- 次のうち1つのコンピュータ
  - HP Compaq Business Desktop dc7100シリーズ
  - HP Compaq Business Desktop dx6100シリーズ
  - HP Compaq Business Desktop d530シリーズ：US、SF、またはMT
  - Compaq Evo D510 US
  - Compaq Evo D510 MT/SF

  BIOSによっては、将来リリースされるコンピュータでもUSBフラッシュ メディア デバイスからの起動がサポートされる場合があります。

注意：上記以外のコンピュータを使用している場合は、コンピュータ セットアップ（F10）ユーティリティに表示されるデフォルトの起動順序で、USBデバイスがハードディスク ドライブより前にあることを確認してください。

- 次のうち1つのストレージ モジュール
  - 16 MB HP USBメモリ
  - 32 MB HP USBメモリ
  - 64 MB HP USBメモリ
  - 128 MB HP USBメモリ
  - 256 MB HP USBメモリ
- FDISKおよびSYSプログラムが格納された、起動可能なDOSディスケット。SYSがない場合はFORMATを使用できますが、USBメモリ上のファイルがすべて失われます。

1. コンピュータの電源を切ります。
2. USBメモリをコンピュータのUSBポートのどれかに差し込み、USBディスケット ドライブ以外のすべてのUSBストレージ デバイスを取り外します。
3. FDISK.COMと、SYS.COMまたはFORMAT.COMのどちらかが格納された起動可能なDOSディスケットをディスケット ドライブに挿入します。コンピュータの電源を入れて、DOSディスケットを起動します。
4. A:¥プロンプトで「**FDISK**」と入力して**[Enter]**キーを押し、FDISKを実行します。メッセージが表示されたら、[Yes (Y)]をクリックして大容量ディスクのサポートを有効にします。
5. 選択肢の「**5**」を入力してコンピュータのドライブを表示します。一覧のドライブの中で最も容量が近いドライブがUSBメモリで、通常は一覧の最後に表示されます。ドライブ名を書き留めておきます。

   USBメモリのドライブ名：_____

注意：ドライブがUSBメモリと一致しない場合は、データの損失を防ぐため、次の手順に進まないでください。他にストレージ デバイスがないか、すべてのUSBポートを確認します。あった場合は取り外してコンピュータを再起動し、手順4に進みます。ない場合、コンピュータがUSBメモリに対応していないか、USBメモリが破損しています。この場合はUSBメモリを起動可能にするための手順を実行しないでください。

6. **[Esc]**キーを押してA:¥プロンプトに戻り、FDISKを終了します。

7. 起動可能なDOSディスケットにSYS.COMがある場合は手順8に、ない場合は手順9に進みます。
8. A:¥プロンプトで「**SYS x:**」（**x**は書き留めたドライブ名）と入力します。

注意：USBメモリのドライブ名を正しく入力したことを確認します。

システム ファイルの転送が完了すると、SYSからA:¥プロンプトに戻ります。手順13に進みます。

9. 保存しておきたいファイルをUSBメモリから別のドライブ（コンピュータの内蔵ハードディスク ドライブなど）の一時ディレクトリにコピーします。
10. A:¥プロンプトで「**FORMAT /S X:**」（**x**は書き留めたドライブ名）と入力します。

注意：USBメモリのドライブ名を正しく入力したことを確認します。

FORMATでは1つ以上の警告が表示され、次の手順に進む前に毎回確認画面が表示されます。毎回「**Y**」と入力します。FORMATによりUSBメモリがフォーマットされ、システム ファイルが追加され、ボリューム ラベルが要求されます。

11. ラベルを付けない場合は**[Enter]**キーを押し、必要な場合はラベルを入力します。
12. 手順9でコピーしたファイルをUSBメモリにコピーしなおします。
13. ディスケットを取り出し、コンピュータを再起動します。USBメモリがCドライブとして起動されます。

デフォルトの起動順序はコンピュータによって異なり、コンピュータ セットアップ（F10）ユーティリティで変更することができます。

Windows 9xからDOSバージョンを使用した場合、短い間Windowsロゴの画面が表示されることがあります。表示されないようにするには、USBメモリのルート ディレクトリにLOGO.SYSというゼロ長のファイルを追加します。

11ページの「複数のコンピュータへのコピー」に戻ります。

サポートされないUSBフラッシュ メディア デバイス

注意：USBフラッシュ メディア デバイスから起動できないコンピュータもあります。コンピュータ セットアップ（F10）ユーティリティに表示されるデフォルトの起動順序で、USBデバイスがハードディスク ドライブより前にある場合、そのコンピュータはUSBフラッシュ メディア デバイスから起動できます。それ以外の場合は、起動可能ディスケットを使用してください。

起動可能なUSBフラッシュ メディア デバイスを作成するには、次のものが必要です。

- 次のうち1つのコンピュータ
  - HP Compaq Business Desktop dc7100シリーズ
  - HP Compaq Business Desktop dx6100シリーズ
  - HP Compaq Business Desktop d530シリーズ：US、SF、またはMT
  - Compaq Evo D510 US
  - Compaq Evo D510 MT/SF

  BIOSによっては、将来リリースされるコンピュータでもUSBフラッシュ メディア デバイスからの起動がサポートされる場合があります。

注意：上記以外のコンピュータを使用している場合は、コンピュータ セットアップ（F10）ユーティリティに表示されるデフォルトの起動順序で、USBデバイスがハードディスク ドライブより前にあることを確認してください。

- FDISKおよびSYSプログラムが格納された、起動可能なDOSディスケット。SYSがない場合はFORMATを使用できますが、USBフラッシュ メディア デバイス上のファイルがすべて失われます。

1. SCSI、ATA RAID、またはSATAドライブが取り付けられたPCIカードがコンピュータにある場合は、コンピュータの電源を切って電源コードを抜き取ります。

注意：電源コードは**必ず**抜き取ってください。

2. コンピュータのカバーを開いてPCIカードを取り外します。

3. USBフラッシュ メディア デバイスをコンピュータのUSBポートのどれかに差し込み、USBディスケット ドライブ以外のすべてのUSBストレージ デバイスを取り外します。コンピュータのカバーを閉じます。
4. 電源コードを差し込んでコンピュータの電源を入れます。
5. コンピュータが起動したらすぐに**[F10]**キーを押したままにし、コンピュータ セットアップを実行します。必要であれば、**[Enter]**キーを押すと、タイトル画面をスキップできます。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータを再起動して、もう一度**[F10]**キーを押したままにしてください。

PS/2キーボードを使用している場合、[Keyboard Error]というメッセージが表示されることがありますが、無視してかまいません。

---

6. **[カスタム]**（Advanced）→**[PCIデバイス]**（PCI Devices）の順に選択してPATAおよびSATAコントローラを無効にします。SATAコントローラを無効にするとき、コントローラに割り当てられているIRQを書き留めておきます。後で再びIRQを割り当てる必要があります。変更を確定して、セットアップ ユーティリティを終了します。

   SATA IRQ：_____

7. FDISK.COMと、SYS.COMまたはFORMAT.COMのどちらかが格納された起動可能なDOSディスケットをディスケット ドライブに挿入します。コンピュータの電源を入れて、DOSディスケットを起動します。
8. FDISKを実行してUSBフラッシュ メディア デバイス上にあるパーティションをすべて削除します。新しいパーティションを作成して有効にします。**[Esc]**キーを押してFDISKを終了します。
9. FDISKを終了してもコンピュータが自動的に再起動されない場合は、**[Ctrl]**＋**[Alt]**＋**[Del]**キーを押して DOSディスケットから起動しなおします。
10. A:¥プロンプトで「**FORMAT C: /S**」と入力し、**[Enter]**キーを押します。FORMATによりUSBフラッシュ メディア デバイスがフォーマットされ、システム ファイルが追加され、ボリューム ラベルが要求されます。
11. ラベルを付けない場合は**[Enter]**キーを押し、必要な場合はラベルを入力します。

12. コンピュータの電源を切って電源コードを抜き取ります。コンピュータのカバーを開き、取り外しておいたPCIカードを取り付けなおします。コンピュータのカバーを閉じます。
13. 電源コードを差し込み、ディスケットを取り出してコンピュータの電源を入れます。
14. コンピュータが起動したらすぐに**[F10]**キーを押したままにし、コンピュータ セットアップを実行します。必要であれば、**[Enter]**キーを押すと、タイトル画面をスキップできます。
15. **[カスタム]**（Advanced）→**[PCIデバイス]**（PCI Devices）の順に選択して、手順6で無効にしたPATAおよびSATAコントローラを再び有効にします。SATAコントローラを元のIRQに割り当てなおします。
16. 変更を保存してユーティリティを終了します。USBフラッシュ メディア デバイスがCドライブとして起動されます。

デフォルトの起動順序はコンピュータによって異なり、コンピュータ セットアップ（F10）ユーティリティで変更することができます。手順については、Documentation CDに収録されている『コンピュータ セットアップ（F10）ユーティリティ ガイド』を参照してください。

Windows 9xからDOSバージョンを使用した場合、短い間Windowsロゴの画面が表示されることがあります。表示されないようにするには、USBフラッシュ メディア デバイスのルート ディレクトリにLOGO.SYSというゼロ長のファイルを追加します。

11ページの「複数のコンピュータへのコピー」に戻ります。

デュアル ステート電源ボタンの設定

お使いのコンピュータでACPI（Advanced Configuration and Power Interface）を使用している場合は、電源ボタンをコンピュータのオン/オフ スイッチとしての機能のほか、スタンバイ モードを起動するためのボタンとして設定することができます。スタンバイ モードでは、電源を完全に切らずに、コンピュータの消費電力を低い状態に保つことができます。使用中のアプリケーションを終了せずに作業を途中で中断したい場合など、スタンバイ モードに設定しておくとコンピュータの電力を低く抑えることができます。

電源ボタンの設定を変更するには、以下の手順で操作します。

1. **[スタート]**ボタンを左クリックし、**[コントロール パネル]**→**[パフォーマンスとメンテナンス]**→**[電源オプション]**の順に選択します。
2. **[電源オプションのプロパティ]**で**[詳細設定]**タブを選択します。
3. **[電源ボタン]**で**[スタンバイ]**を選択します。

電源ボタンにスタンバイ ボタンとしての機能を設定してある場合は、コンピュータの電源が入っているときに電源ボタンを押すと、スタンバイ モードを起動することができます。再び電源ボタンを押すと、直ちにスタンバイ モードから復帰できます。コンピュータの電源を完全に切るには、電源ボタンを4秒以上押し続けます。

注意：システムが応答しない場合以外は、電源ボタンを使って電源を切らないでください。オペレーティング システムを通さずに電源を切ると、ハード ディスク ドライブが破損したりデータが損失したりする可能性があります。

インターネットWebサイト

HPの技術者はHP製および他社製のソフトウェアのテストおよび修正を厳密に行い、オペレーティング システムに特化したサポート ソフトウェアを開発しています。このため、HPのコンピュータは優れた性能、互換性、および信頼性を兼ね備えています。

別の種類のオペレーティング システムをインストールしたり新しいバージョンのオペレーティング システムに移行したりする場合、それぞれのオペレーティング システム用に設計されたサポート ソフトウェアを実行してください。お使いのコンピュータにインストールされているバージョンと異なるバージョンのMicrosoft Windowsを実行したい場合、対応するデバイス ドライバおよびユーティリティをインストールして、すべての機能がサポートされ、正しく動作することを確認してください。

HPでは、快適な環境で効率的にコンピュータをお使いいただくために、最新のデバイス ドライバ、ユーティリティ、フラッシュ ROMイメージなどを収録したサポート ソフトウェアを提供しています。サポート ソフトウェアはHPのWebサイト（http://www.hp.com/support）からダウンロードできます。

HPのホームページには、HP製のコンピュータでMicrosoft Windowsのオペレーティング システムを実行する際に必要な最新のデバイス ドライバ、ユーティリティ、フラッシュ ROMイメージなどが用意されています。

標準規格およびパートナー企業

HPのインテリジェント マネジメント機能は、各社のシステム マネジメント アプリケーションを取り入れており、次のようなコンピュータ業界の標準規格に準拠しています。

- Web-Based Enterprise Management（WBEM）
- Windows Management Interface（WMI）
- Wake on LANテクノロジ
- ACPI
- SMBIOS
- Pre-boot Execution（PXE）サポート

資産情報管理機能およびセキュリティ機能

コンピュータに搭載される資産情報管理機能を使用すれば、HP Systems Insightマネージャ、HP Client Manager、またはその他のシステム管理アプリケーションを使用して管理される資産情報を確認することができます。資産情報管理機能とこれらの管理ソフトウェア製品を統合することにより、お使いの環境に最適な管理ソフトウェアを選択でき、今までお使いになっていたソフトウェアをより有効に活用できます。

さらに、HPでは、コンピュータとデータを不正なアクセスから保護するための機能を備えています。HP ProtectTools内蔵セキュリティがインストールされている場合は、データへの不正なアクセスの防止、システムの整合性の確認、および第三者からのアクセスに対する認証が行われます。（詳しくは、Documentation CDに収録されている『HP ProtectTools内蔵セキュリティ ガイド』を参照してください。）一部のモデルに装備されているProtectTools、スマート カバー センサ/カバー リムーバル センサ（Cover Removal Sensor）、およびスマート カバー ロック（Smart Cover Lock）のようなセキュリティ機能は、コンピュータの内部装置への不正なアクセスの防止に役立ちます。パラレル ポート、シリアル ポート、またはUSBポートを無効にすることにより、またリムーバブル メディア ブート機能を無効にすることにより、貴重な資産であるデータを保護できます。これ以外にも、メモリ脱着センサおよびスマート カバー センサ/カバー リムーバル センサからの警告が自動的にシステム管理アプリケーションに転送されることで、コンピュータの内部装置への不正なアクセスを防ぐことができます。

ProtectTools、スマート カバー センサ/カバー リムーバル センサ、およびスマート カバー ロックは、一部のシステムにオプションとして装備されています。

次のユーティリティを使用して、セキュリティ機能の設定を管理できます。

- コンピュータ セットアップ（F10）ユーティリティを使用してローカルで管理します。コンピュータ セットアップ（F10）ユーティリティの詳しい情報と手順については、コンピュータに付属のDocumentation CDに収録されている『コンピュータ セットアップ（F10）ユーティリティ ガイド』を参照してください。

- HP Client Manager SoftwareまたはSystem Software Managerを使用してリモートで管理します。このソフトウェアにより、簡単なコマンドラインユーティリティを使用して、ネットワークのセキュリティ機能の設定を確実に、一貫して集中管理することができます。

次の表と各項で、コンピュータ セットアップ（F10）ユーティリティを使ってローカルでコンピュータのセキュリティ機能を管理する方法を説明します。

セキュリティ機能

項目	説明
セットアップ パスワード (Setup Password)	セットアップ（管理者）パスワードを設定して有効にします ✎ セットアップ パスワードを設定すると、コンピュータ セットアップ ユーティリティの設定を変更したり、ROMをフラッシュしたり、Windows環境で特定のプラグ アンド プレイ設定を変更したりする場合にセットアップ パスワードが必要になります 詳しくは、Documentation CDに収録されている『トラブルシューティング ガイド』を参照してください
電源投入時パスワード (Power-On Password)	電源投入時パスワードを設定して有効にします 詳しくは、Documentation CDに収録されている『トラブルシューティング ガイド』を参照してください
パスワード オプション (Password Options) (電源投入時パスワードが設定されている場合にのみ表示されます)	ウォーム ブート（**[Ctrl]**+**[Alt]**+**[Delete]**）にパスワードが必要かどうかを指定します 詳しくは、Documentation CDに収録されている『デスクトップ マネジメントについて』を参照してください
起動前の承認 (Pre-Boot Authorization)	電源投入時パスワード（Power-On Password）の代わりにスマート カードを使用することを有効/無効にします
スマート カバー (Smart Cover)	次の項目を設定します • カバー ロック（Cover Lock）の有効（Enable）/無効（Disable）の設定 • カバー リムーバル センサの有効/無効の設定 ✎ [ユーザに通知]を設定すると、カバーが取り外されたことをセンサが検知したときにユーザに通知されます。セットアップ パスワードは、カバーが取り外されたことをセンサが検知した場合、コンピュータを起動する際にセットアップ パスワードの入力を要求します 一部のモデルでのみサポートされます。詳しくは、34ページの「スマート カバー センサ/カバー リムーバル センサ （Cover Removal Sensor）」を参照してください

✎ コンピュータ セットアップについて詳しくは、Documentation CDに収録されている『コンピュータ セットアップ（F10）ユーティリティ ガイド』を参照してください。サポートされるセキュリティ機能は、お使いのコンピュータの構成によって異なる場合があります。

セキュリティ機能（続き）

項目	説明
内蔵セキュリティ (Embedded Security)	次の項目を設定します • 内蔵セキュリティ デバイスの有効（Enable）/無効（Disable） • デバイスの出荷時設定へのリセット 一部のモデルでのみサポートされます。詳しくは、Documentation CDに収録されている『HP ProtectTools内蔵セキュリティ ガイド』を参照してください
デバイス セキュリティ (Device Security)	シリアル ポート（Serial Port）、パラレル ポート（Parallel Port）、前面のUSBポート（Front USB Port）、システムのオーディオ セキュリティ（Audio Security）、モデルによってはネットワーク コントローラ（Network Controller）、マルチベイ デバイス（Multibay Devices）、およびSCSIコントローラ（SCSI Controller）のデバイス有効（Enable）/デバイス無効（Disable）の設定
ネットワーク サービス ブート (Network Service Boot)	ネットワーク サーバにインストールされたオペレーティング システムからコンピュータを起動する機能の有効（Enable）/無効（Disable）の設定（NICモデルのみで使用でき、ネットワーク コントローラがPCIバス上に存在するか、システム ボードに組み込まれている必要があります）
システムID (System ID)	次の項目を設定します • アセット タグ（Asset Tag。18バイトのID）およびオーナーシップ タグ（Ownership Tag。POST実行中に表示される80バイトのID）の入力 詳しくは、Documentation CDに収録されている『デスクトップ マネジメントについて』を参照してください • 本体シリアル番号（Chassis Serial Number）またはUUID（Universal Unique Identifier）の入力 UUIDは現在の本体シリアル番号が無効の場合にのみ更新できます（通常これらの識別（ID）番号は工場出荷時に設定され、そのシステムを特定するために使用されます） • キーボード（Keyboard Locale）の設定 英語用やドイツ語用などをシステムIDエントリに対して設定します

✎ コンピュータ セットアップについて詳しくは、Documentation CDに収録されている『コンピュータ セットアップ（F10）ユーティリティ ガイド』を参照してください。サポートされるセキュリティ機能は、お使いのコンピュータの構成によって異なる場合があります。

セキュリティ機能（続き）

項目	説明
ドライブロック （DriveLock）	マルチベイ ハードディスク ドライブにマスタ パスワードまたはユーザ パスワードを割り当てたり、パスワードを変更したりします（SCSIハードディスク ドライブではサポート されません）。この機能が有効の場合は、POST実行中にどちらかのDriveLockパスワードを入力するよう求められます。どちらのパスワードも正常に入力されなかった場合は、次のコールド ブート シーケンスの間にどちらかのパスワードが入力されるまで、ハードディスク ドライブにはアクセスできません ✎ この項目は、DriveLock機能をサポートする1台以上のマルチベイ ハードディスク ドライブがシステムに接続されている場合にのみ表示されます 詳しくは、Documentation CDに収録されている『デスクトップ マネジメントについて』を参照してください
マスタ ブート レコード セキュリティ （Master Boot Record Security）	マスタ ブート レコード（MBR）セキュリティを有効（Enable）/無効（Disable）に設定します 有効に設定すると、BIOSは、現在の起動可能ディスクのMBRへの書き込み要求をすべて拒否します。コンピュータの電源を入れるか再起動するたびに、BIOSは現在の起動可能ディスクのMBRと前回保存したMBRとを比較します。変更が検出された場合、現在の起動可能ディスクのMBRを保存するか、前回保存したMBRを復元するか、またはMBRセキュリティを無効にすることができます。セットアップ パスワードが設定されている場合は、セットアップ パスワードを入力する必要があります ✎ 現在の起動可能ディスクのフォーマットやパーティションを意図的に変更する際は、MBRセキュリティを無効に設定します。一部のディスク ユーティリティ（FDISKやFORMATなど）はMBRを更新しようとします MBRセキュリティが有効に設定されたままBIOSによってディスク アクセスの処理が行われると、MBRへの書き込み要求は拒否され、ユーティリティはエラーを表示します MBRセキュリティが有効に設定されたままオペレーティング システムによってディスク アクセスの処理が行われると、次の再起動時にBIOSによってMBRの変更が検出され、MBRセキュリティの警告メッセージが表示されます

✎ コンピュータ セットアップについて詳しくは、Documentation CDに収録されている『コンピュータ セットアップ（F10）ユーティリティ ガイド』を参照してください。サポートされるセキュリティ機能は、お使いのコンピュータの構成によって異なる場合があります。

セキュリティ機能（続き）

項目	説明
マスタ ブート レコードの保存 （Save Master Boot Record）	現在の起動可能ディスクのマスタ ブート レコードのバックアップ コピーを保存します MBRセキュリティが有効の場合にのみ表示されます
マスタ ブート レコードの復元 （Restore Master Boot Record）	マスタ ブート レコードのバックアップを現在の起動可能ディスクに復元します 次の条件がすべて満たされている場合にのみ表示されます • MBR セキュリティが有効に設定されている • 以前に MBR のバックアップ コピーが保存されている • 現在の起動可能ディスクが、MBR のバックアップ コピーを保存したときのディスクと同じである **注意：**通常は、ディスク ユーティリティやオペレーティング システムからMBRが変更された後に、以前保存しておいたMBRのバックアップを復元すると、ディスク上のデータにアクセスできなくなる可能性があります。現在の起動可能ディスクのMBRが壊れているかウィルスに感染していることが確実な場合にのみ、バックアップ コピーを復元してください

コンピュータ セットアップについて詳しくは、Documentation CDに収録されている『コンピュータ セットアップ（F10）ユーティリティ ガイド』を参照してください。サポートされるセキュリティ機能は、お使いのコンピュータの構成によって異なる場合があります。

パスワードのセキュリティ

電源投入時パスワード（Power-on password）を設定すると、コンピュータの電源を入れたり再起動したりするたびに、アプリケーションやデータにアクセスするためのパスワードの入力が要求されるので、コンピュータが許可無く使用されることを防止できます。セットアップ パスワード（Setup password）は、特にコンピュータ セットアップ（F10）ユーティリティへの不正アクセスを防ぎます。セットアップ パスワードを、電源投入時パスワードの補助手段として使用することもできます。つまり、電源投入時パスワードの入力を要求されたときに、代わりにセットアップ パスワードを入力してコンピュータにアクセスすることもできます。

ネットワーク全体のセットアップ パスワードを設定しておくと、システム管理者はネットワーク上のすべてのシステムにログインでき、設定されている電源投入時パスワードを知らなくてもメンテナンスを行うことができます。

セットアップ パスワードの設定

システムに内蔵セキュリティ デバイスが搭載されている場合は、Documentation CDに収録されている『HP ProtectTools内蔵セキュリティ ガイド』を参照してください。**[コンピュータ セットアップ**（F10）**ユーティリティ]**メニューで、セットアップ パスワードを設定しておけば、無断でコンピュータの設定が変更されることを防止できます。

1. コンピュータの電源を入れるか、**[スタート]**→**[シャットダウン]**→**[再起動]**→[OK]の順に選択して再起動します。
2. コンピュータが起動したらすぐに**[F10]**キーを押したままにし、コンピュータ セットアップを実行します。必要であれば、**[Enter]**キーを押すと、タイトル画面をスキップできます。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータを再起動して、もう一度**[F10]**キーを押したままにしてください。

PS/2キーボードを使用している場合、[Keyboard Error]というメッセージが表示されることがありますが、無視してかまいません。

3. **[セキュリティ]**（Security）→**[セットアップ パスワード]**（Setup Password）の順に選択したあと、画面上のメッセージに従って操作します。
4. 設定を終了するには、**[ファイル]**（File）→**[変更を保存して終了]**（Save Changes and Exit）の順に選択します。

電源投入時パスワードの設定

[コンピュータ セットアップ ユーティリティ]メニューで、電源投入時パスワードを設定しておけば、無断でコンピュータが使用されることを防止できます。電源投入時パスワードが設定されていると、コンピュータ セットアップ ユーティリティの**[セキュリティ設定]**（Security）メニューに**[パスワード オプション]**（Password Options）が表示されます。パスワード オプションには**[ウォーム ブート時のパスワード入力]**（Password Prompt on Warm Boot）などが含まれます。**[ウォーム ブート時のパスワード入力]**が有効にされている場合も、コンピュータを再起動するたびにパスワードを入力する必要があります。

1. コンピュータの電源を入れるか、**[スタート]**→**[シャットダウン]**→**[再起動]**→[OK]の順に選択して再起動します。
2. コンピュータが起動したらすぐに**[F10]**キーを押したままにし、コンピュータ セットアップを実行します。必要であれば、**[Enter]**キーを押すと、タイトル画面をスキップできます。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータを再起動して、もう一度**[F10]**キーを押したままにしてください。

PS/2キーボードを使用している場合、[Keyboard Error]というメッセージが表示されることがありますが、無視してかまいません。

3. **[セキュリティ]**→**[電源投入時パスワード]**（Power-On Password）の順に選択したあと、画面上のメッセージに従って操作します。
4. 設定を終了するには、**[ファイル]**（File）→**[変更を保存して終了]**（Save Changes and Exit）の順に選択します。

電源投入時パスワードの入力

電源投入時パスワードを入力するには、以下の手順で操作します。

1. コンピュータの電源を入れるか、**[スタート]**→**[シャットダウン]**→**[再起動]**→[OK]の順に選択して再起動します。
2. 鍵形のアイコンが表示されたら、パスワードを入力して**[Enter]**キーを押します。

機密保護のため、入力したパスワードは画面に表示されません。パスワードを入力する際は、間違えないよう注意してください。

間違ったパスワードを入力した場合は、鍵形に×印のついたアイコンが表示されますので、パスワードを正しく入力しなおしてください。続けて3回間違えた場合は、コンピュータの電源をいったん切って最初から操作しなおす必要があります。

セットアップ パスワードの入力

システムに内蔵セキュリティ デバイスが搭載されている場合は、Documentation CDに収録されている『HP ProtectTools内蔵セキュリティ ガイド』を参照してください。

コンピュータでセットアップ パスワードを設定しておけば、**[コンピュータ セットアップ ユーティリティ]**メニューを実行するたびに、必ずパスワードの入力が必要となります。

1. コンピュータの電源を入れるか、**[スタート]→[シャットダウン]→[再起動]**→[OK]の順に選択して再起動します。
2. コンピュータが起動したらすぐに**[F10]**キーを押したままにし、コンピュータ セットアップを実行します。必要であれば、**[Enter]**キーを押すと、タイトル画面をスキップできます。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータを再起動して、もう一度**[F10]**キーを押したままにしてください。

PS/2キーボードを使用している場合、[Keyboard Error]というメッセージが表示されることがありますが、無視してかまいません。

3. 鍵形のアイコンが表示されたら、セットアップ パスワードを入力して**[Enter]**キーを押します。

機密保護のため、入力したパスワードは画面に表示されません。パスワードを入力する際は、間違えないよう注意してください。

間違ったパスワードを入力した場合は、鍵形に×印のついたアイコンが表示されますので、パスワードを正しく入力しなおしてください。続けて3回間違えた場合は、コンピュータの電源をいったん切って最初から操作しなおす必要があります。

電源投入時パスワードまたはセットアップ パスワードの変更

システムに内蔵セキュリティ デバイスが搭載されている場合は、Documentation CDに収録されている『HP ProtectTools内蔵セキュリティ ガイド』を参照してください。

1. コンピュータの電源を入れるか、**[スタート]→[シャットダウン]→[再起動]**→[OK]の順に選択して再起動します。
2. 電源投入時パスワードを変更する場合は、手順3に進みます。

   セットアップ パスワードを変更する場合は、コンピュータが起動したらすぐに**[F10]**キーを押したままにし、コンピュータ セットアップを実行します。必要であれば、**[Enter]**キーを押すと、タイトル画面をスキップできます。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータを再起動して、もう一度**[F10]**キーを押したままにしてください。

PS/2キーボードを使用している場合、[Keyboard Error]というメッセージが表示されることがありますが、無視してかまいません。

---

3. 鍵形のアイコンが表示されたら、次のように入力します。

   現在のパスワード/新しいパスワード/新しいパスワード

機密保護のため、入力したパスワードは画面に表示されません。パスワードを入力する際は、間違えないよう注意してください。

---

4. **[Enter]**キーを押します。

新しいパスワードは、次にコンピュータの電源を入れたときから有効になります。

電源投入時パスワードとセットアップ パスワードは、コンピュータ セットアップ（F10）ユーティリティの**[セキュリティ]**（Security）オプションを使って変更することもできます。

電源投入時パスワードまたはセットアップ パスワードの削除

システムに内蔵セキュリティ デバイスが搭載されている場合は、Documentation CDに収録されている『HP ProtectTools内蔵セキュリティ ガイド』を参照してください。

1. コンピュータの電源を入れるか、**[スタート]→[シャットダウン]→[再起動]→[OK]**の順に選択して再起動します。
2. 電源投入時パスワードを削除する場合は、手順3に進みます。

   セットアップ パスワードを削除する場合は、コンピュータが起動したらすぐに**[F10]**キーを押したままにし、コンピュータ セットアップを実行します。必要であれば、**[Enter]**キーを押すと、タイトル画面をスキップできます。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータを再起動して、もう一度**[F10]**キーを押したままにしてください。

PS/2キーボードを使用している場合、[Keyboard Error]というメッセージが表示されることがありますが、無視してかまいません。

3. 鍵形のアイコンが表示されたら、次のように入力します。

   現在のパスワード/

4. **[Enter]**キーを押します。

電源投入時パスワードとセットアップ パスワードは、コンピュータ セットアップ ユーティリティの**[セキュリティ]**（Security）オプションを使って変更することもできます。

電源投入時パスワードを忘れてしまった場合

設定しておいた電源投入時パスワードを忘れると、コンピュータを使用できなくなります。パスワードを解除する方法については、Documentation CDに収録されている『トラブル シューティング ガイド』を参照してください。

システムに内蔵セキュリティ デバイスが搭載されている場合は、Documentation CDに収録されている『HP ProtectTools内蔵セキュリティ ガイド』を参照してください。

ドライブロック（DriveLock）

ドライブロックは、マルチベイ ハードディスク ドライブにあるデータへの不正アクセスを防止する業界標準のセキュリティ機能であり、コンピュータ セットアップ（F10）ユーティリティの拡張機能として実装されています。この機能は、ドライブロックが可能なハードディスク ドライブが検出された場合にのみ利用できます。

ドライブロックは、データのセキュリティを最重要視するユーザ向けに開発されました。このようなユーザにとっては、ハードディスク ドライブのコストとそこに格納されているデータの喪失は、データへの不正アクセスの結果生じる可能性のある損害に比べれば、些細なものです。このレベルのセキュリティの確保と同時に、パスワードを忘れたときの対処もできるように、HP が実装したドライブロックでは、2つのパスワードによるセキュリティ方式を採用しています。一方のパスワードはシステム管理者が設定して使用するもので、もう一方のパスワードは通常、エンド ユーザが設定して使用します。両方のパスワードを忘れてしまった場合にドライブをアンロックするための手段はありません。したがって、ハードディスク ドライブに含まれるデータが企業情報システムに複製されているか、または定期的にバックアップが作成されている場合に、ドライブロックを最も安全に使用できます。

ドライブロックの両方のパスワードを忘れてしまった場合は、ハードディスク ドライブを使用できなくなります。前に述べたカスタマ プロファイルに適合しないすべてのユーザにとって、この事実は受け入れ難いリスクになる可能性があります。一方、カスタマ プロファイルに適合するユーザにとっては、ハードディスク ドライブに保存されたデータの性質上、許容できるリスクだと言えます。

ドライブロックの使用法

[ドライブロック]（DriveLock）オプションは、コンピュータ セットアップ（F10）ユーティリティの**[セキュリティ]**（Security）メニューに表示されます。ユーザには、マスタ パスワード（master password）を設定したりドライブロックを有効にしたりするオプションが提供されます。ドライブロックを有効にするには、ユーザ パスワード（user password）を入力する必要があります。通常、ドライブロックの最初のコンフィギュレーションはシステム管理者が実行するので、マスタ パスワードを最初に設定する必要があります。ドライブロックを有効にするか無効のままにしておくかにかかわらず、管理者はマスタ パスワードを設定することをお勧めします。これにより、将来ドライブがロックされた場合に、管理者はドライブロックの設定値を変更できるようになります。マスタ パスワードが設定されると、システム管理者はいつでもドライブロックを有効にしたり無効にしたりすることができます。

ロックされたハードディスク ドライブが存在する場合は、POST（Power-On Self Test）によって、そのドライブをアンロックするためのパスワードが要求されます。電源投入時パスワード（power-on password）が設定されていて、そのドライブのユーザ パスワードと一致する場合は、パスワードの再入力は要求されません。一致しない場合は、ドライブロックのパスワードを入力するよう要求されます。マスタ パスワードとユーザ パスワードのどちらを使うこともできます。ユーザは、パスワードが正しいと認識されるまで、2回入力できます。2回とも受け入れられない場合でもPOSTは続行されますが、そのドライブにはアクセスできません。

ドライブロックの使用例

ドライブロックのセキュリティ機能は、企業環境での使用に最も適しています。つまり、システム管理者が、ユーザに複数のコンピュータで使用できるようマルチベイ ハードディスク ドライブを提供する場合です。システム管理者はマルチベイ ハードディスク ドライブのコンフィギュレーションを担当しますが、その作業には、ドライブロックのマスタ パスワードを設定することが含まれます。ユーザがユーザ パスワードを忘れた場合や、コンピュータを別の従業員が使うことになった場合、システム管理者はマスタ パスワードを使用して、ユーザ パスワードをリセットしたり、ハードディスク ドライブへのアクセス権を回復したりすることができます。

企業システム管理者は、ドライブロックを有効にする場合、マスタ パスワードの設定とメンテナンスについての企業方針を確立しておくことをお勧めします。これは、従業員が会社を辞める前に意図的に、または誤ってドライブロックの両方のパスワードを設定してしまうという状況を防ぐために必要です。両方のパスワードを設定した従業員が会社を辞めてしまった場合、そのハードディスク ドライブは使用不能となり、交換が必要になります。また、マスタ パスワードが設定されていないと、システム管理者がロックされたハードディスク ドライブにアクセスできなくなり、不正ソフトウェアの日常チェックや、その他の資産管理およびサポートを実行できなくなることがあります。

それほど厳重なセキュリティを必要としないユーザの場合は、ドライブロックを有効にしないことをお勧めします。この種のユーザには、個人ユーザや、機密性の高いデータをハードディスク ドライブに保持しないことを習慣にしているユーザが含まれます。このようなユーザにとっては、両方のパスワードを忘れてハードディスク ドライブが使えなくなることのほうが、ドライブロックにより保護されるデータの価値よりもはるかに大きな問題と言えます。コンピュータ セットアップ（F10）ユーティリティとドライブロックへのアクセスは、セットアップ パスワードによって制限できます。セットアップ パスワードを指定してそれをエンド ユーザに公表しないことで、システム管理者はユーザがドライブロックを有効にできないようにします。

スマート カバー センサ/カバー リムーバル センサ（Cover Removal Sensor）

一部のモデルに搭載されているスマート カバー センサ/カバー リムーバル センサとは、本体のカバーまたはサイド パネルの着脱があったことをユーザに知らせる、ハードウェア技術とソフトウェア技術を結合した機能です。3段階の設定レベルがあり、本体のカバーの着脱があった後で初めてコンピュータの電源を入れたときの動作が異なります。

スマート カバー センサ/カバー リムーバル センサの動作

レベル	設定	コンピュータ起動時の動作
0	[無効]（Disabled）	スマート カバー センサ/カバー リムーバル センサは無効（デフォルト）
1	[ユーザに通知]（Notify User）	本体のカバーが取り外されたことを知らせるメッセージが画面に表示される
2	[セットアップ パスワード]（Setup Password）	本体のカバーが取り外されたことを知らせるメッセージが画面に表示される セットアップ パスワードを入力するまで、コンピュータを使用できない

これらの設定は、コンピュータ セットアップを使用して変更できます。コンピュータ セットアップについて詳しくは、Documentation CDに収録されている『コンピュータ セットアップ（F10）ユーティリティ ガイド』を参照してください。

スマート カバー センサ/カバー リムーバル センサ（Cover Removal Sensor）の保護レベルの設定

スマート カバー センサ/カバー リムーバル センサ機能を有効に設定するには、以下の手順で操作します。

1. コンピュータの電源を入れるか、**[スタート]→[シャットダウン]→[再起動]**→[OK]の順に選択して再起動します。
2. コンピュータが起動したらすぐに**[F10]**キーを押したままにし、コンピュータ セットアップを実行します。必要であれば、**[Enter]**キーを押すと、タイトル画面をスキップできます。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータを再起動して、もう一度**[F10]**キーを押したままにしてください。

PS/2キーボードを使用している場合、[Keyboard Error]というメッセージが表示されることがありますが、無視してかまいません。

3. **[セキュリティ]**（Security）→**[スマート カバー]**（Smart Cover）→**[カバー リムーバル センサ]**（Cover Removal Sensor）の順に選択した後、必要なセキュリティ レベルを選択します。
4. 設定を終了するには、**[ファイル]**（File）→**[変更を保存して終了]**（Save Changes and Exit）の順に選択します。

スマート カバー ロック

スマート カバー ロックは、コンピュータのカバーのロックをソフトウェアで制御する、一部のHPのコンピュータでサポートされる機能です。スマート カバー ロックを使用して、コンピュータ内部の装置への不正なアクセスを防ぎます。工場出荷時には、ロックが解除された状態になっています。

注意: スマート カバー ロックを使用する場合は、必ずセットアップ パスワードを設定して、無断でロックを解除できないようにしておいてください。

スマート カバー ロックは、一部のシステムにオプションとして装備されています。

スマート カバー ロックの設定

スマート カバー ロックを使ってコンピュータ本体のカバーをロックするには、以下の手順で操作します。

1. コンピュータの電源を入れるか、**[スタート]→[シャットダウン]→[再起動]→[OK]**の順に選択して再起動します。
2. コンピュータが起動したらすぐに**[F10]**キーを押したままにし、コンピュータ セットアップを実行します。必要であれば、**[Enter]**キーを押すと、タイトル画面をスキップできます。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータを再起動して、もう一度**[F10]**キーを押したままにしてください。

PS/2キーボードを使用している場合、[Keyboard Error]というメッセージが表示されることがありますが、無視してかまいません。

---

3. **[セキュリティ]**（Security）→**[スマート カバー]**（Smart Cover）→**[カバー ロック]**（Cover Lock）→**[ロック]**（Lock）の順に選択します。
4. 設定を終了するには、**[ファイル]**（File）→**[変更を保存して終了]**（Save Changes and Exit）の順に選択します。

スマート カバー ロックの解除

1. コンピュータの電源を入れるか、**[スタート]→[シャットダウン]→[再起動]→[OK]**の順に選択して再起動します。
2. コンピュータが起動したらすぐに**[F10]**キーを押したままにし、コンピュータ セットアップを実行します。必要であれば、**[Enter]**キーを押すと、タイトル画面をスキップできます。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータを再起動して、もう一度**[F10]**キーを押したままにしてください。

PS/2キーボードを使用している場合、[Keyboard Error]というメッセージが表示されることがありますが、無視してかまいません。

---

3. **[セキュリティ]→[スマート カバー]→[カバー ロック]→[アンロック]**（Unlock）の順に選択します。
4. 設定を終了するには、**[ファイル]→[変更を保存して終了]**の順に選択します。

Smart Cover FailSafeキーの使用

スマート カバー ロックを使ってコンピュータをロックしたまま、パスワードを入力できなくなってしまった場合、Smart Cover FailSafeキーを使用して、コンピュータ本体のカバーを開ける必要があります。Smart Cover FailSafe キーが必要となるのは、次のような場合です。

- 停電
- 起動障害
- コンピュータ部品（プロセッサや電源など）の障害
- パスワードを忘れてしまった場合

注意：Smart Cover FailSafeキーは、HPが提供する専用ツールです。必要になる前に、HP製品販売店であらかじめご用意いただくことをお勧めします。

Smart Cover FailSafeキーの入手については、HPのサポート窓口にお問い合わせください。

Smart Cover FailSafeキーについて詳しくは、Documentation CDに収録されている『ハードウェア リファレンス ガイド』を参照してください。

マスタ ブート レコード セキュリティ（Master Boot Record Security）

マスタ ブート レコード（MBR）には、ディスクから正常に起動して、ディスク上に保存されているデータにアクセスするための情報が入っています。マスタ ブート レコードのセキュリティ機能によって、誤ってMBRを変更したり不正にMBRが変更されたりすると（一部のコンピュータ ウイルスによってデータが変更されたり、ディスク ユーティリティを誤って使用したりするなど）、その変更が検出および報告されます。また、システムの再起動時にMBRへの変更が検出された場合、このセキュリティによって「正常であることが分かっている最新の」MBRを復元することができます。

MBRセキュリティを有効にするには、以下の手順で操作します。

1. コンピュータの電源を入れるか、**[スタート]→[シャットダウン]→[再起動]**→[OK]の順に選択して再起動します。
2. コンピュータが起動したらすぐに**[F10]**キーを押したままにし、コンピュータ セットアップを実行します。必要であれば、**[Enter]**キーを押すと、タイトル画面をスキップできます。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータを再起動して、もう一度**[F10]**キーを押したままにしてください。

PS/2キーボードを使用している場合、[Keyboard Error]というメッセージが表示されることがありますが、無視してかまいません。

3. **[セキュリティ]**（Security）→**[マスタ ブート レコード セキュリティ]**（Master Boot Record Security）→**[有効]**（Enabled）の順に選択します。
4. **[セキュリティ]→[マスタ ブート レコードの保存]**（Save Master Boot Record）の順に選択します。
5. 設定を終了するには、**[ファイル]**（File）→**[変更を保存して終了]**（Save Changes and Exit）の順に選択します。

MBRセキュリティを有効にすると、BIOSは、MS-DOSやWindowsのSafeモードで現在の起動可能ディスクのMBRが変更されることを防ぎます。

ほとんどのオペレーティング システムは、現在の起動可能ディスクのMBRへのアクセスを制御します。したがって、オペレーティング システムの動作中に行われる変更については、BIOSは阻止できません。

コンピュータの電源を入れるか、再起動するたびに、BIOSは現在の起動可能ディスクのMBRと前回に保存されたMBRとを比較します。変更が検出され、かつ現在の起動可能ディスクが、前回MBRを保存したディスクと同じである場合、次のメッセージが表示されます。

1999 - Master Boot Record has changed.（マスタ ブート レコードが変更されました。）

Press any key to enter Setup to configure MBR Security.（任意のキーを押して**[コンピュータ セットアップ ユーティリティ]**メニューで、MBRセキュリティを設定してください。）

[コンピュータ セットアップ ユーティリティ]メニューで、次のどれかの操作を行います。

- 現在の起動可能ディスクのMBRを保存します。
- 前回保存したMBRを復元します。または、
- MBRセキュリティ機能を無効にします。

セットアップ パスワードが設定されている場合は、セットアップ パスワードの入力が必要です。

変更が検出され、現在の起動可能ディスクが、前回にMBRを保存したディスクと同じで**ない**場合は、次のメッセージが表示されます。

2000 - Master Boot Record Hard Drive has changed.（マスタ ブート レコードのハードディスク ドライブが変更されています。）

Press any key to enter Setup to configure MBR Security.（任意のキーを押して**[コンピュータ セットアップ ユーティリティ]**メニューで、MBRセキュリティを設定してください。）

[コンピュータ セットアップ ユーティリティ]メニューで、次のどちらかの操作を行います。

- 現在の起動可能ディスクのMBRを保存します。または、
- MBRセキュリティ機能を無効にします。

セットアップ パスワードが設定されている場合は、セットアップ パスワードの入力が必要です。

万一、前回保存したMBRが破損した場合は、次のメッセージが表示されます。

1998 - Master Boot Record has been lost.（マスタ ブート レコードがありません。）

Press any key to enter Setup to configure MBR Security.（任意のキーを押して**[コンピュータ セットアップ ユーティリティ]**メニューで、MBRセキュリティを設定してください。）

[コンピュータ セットアップ ユーティリティ]メニューで、次のどちらかの操作を行います。

- 現在の起動可能ディスクのMBRを保存します。または、
- MBRセキュリティ機能を無効にします。

セットアップ パスワードが設定されている場合は、セットアップ パスワードの入力が必要です。

現在の起動可能ディスクのパーティションとフォーマットを変更する前に

現在の起動可能ディスクのパーティションやフォーマットを変更する前に、MBR セキュリティが無効になっていることを確認してください。FDISK や FORMAT など一部のディスク ユーティリティは、MBR を更新しようとします。ディスクのパーティションやフォーマットを変更する際にMBRセキュリティが有効である場合は、次にコンピュータの電源を入れるか再起動したときに、ディスク ユーティリティからエラー メッセージが表示されたり、MBR セキュリティから警告が発生したりする可能性があります。MBR セキュリティを無効にするには、以下の手順で操作します。

1. コンピュータの電源を入れるか、**[スタート]→[シャットダウン]→[再起動]→[OK]**の順に選択して再起動します。
2. コンピュータが起動したらすぐに**[F10]**キーを押したままにし、コンピュータ セットアップを実行します。必要であれば、**[Enter]**キーを押すと、タイトル画面をスキップできます。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータを再起動して、もう一度**[F10]**キーを押したままにしてください。

PS/2キーボードを使用している場合、[Keyboard Error]というメッセージが表示されることがありますが、無視してかまいません。

3. **[セキュリティ]**（Security）→**[マスタ ブート レコード セキュリティ]**（Master Boot Record Security）→**[無効]**（Disabled）の順に選択します。
4. 設定を終了するには、**[ファイル]**（File）→**[変更を保存して終了]**（Save Changes and Exit）の順に選択します。

ケーブル ロックの取り付け

コンピュータのリア パネルにはケーブル ロックを取り付けられるようになっているので、市販のケーブル ロックを使用して、コンピュータを作業エリアに固定できます。

詳しくは、Documentation CDに収録されている『ハードウェア リファレンス ガイド』を参照してください。

指紋認証テクノロジ

HP指紋認証テクノロジを使用すると、エンド ユーザのパスワードの入力が不要となるため、ネットワークのセキュリティを強化する一方で、ログイン手順を簡素化し、企業のネットワーク管理に関わる経費を削減することができます。また、手頃な価格のため、もはや一部のハイテク産業や高度なセキュリティを扱う組織や企業だけのものではなくなりました。

モデルによっては、指紋認証テクノロジがサポートされていない場合があります。

詳しくは、次のWebサイト（英語サイト）を参照してください。

http://h18004.www1.hp.com/products/security/

障害通知および復旧機能

障害通知および復旧機能とは、最新のハードウェア/ソフトウェア技術を結合して、重要なデータの損失を防ぎ、故障時間を最小限に抑える機能です。

HP Client Managerによって管理されるネットワークにコンピュータが接続されている場合、ネットワーク管理ソフトウェアに障害通知が送られます。HP Client Manager Softwareでは、管理されているすべてのコンピュータで診断ユーティリティを実行し、失敗したテストの概要を作成するよう、リモートでスケジュールを設定することもできます。

ドライブ保護システム

ドライブ保護システム（DPS）は、一部のモデルに搭載されたハードディスクドライブに組み込まれている診断ツールです。DPSを使用して、保証規定が適用されない、ハードディスク ドライブの交換に至るような問題を診断します。

コンピュータの組み立て時に各ハードディスク ドライブに対してDPSテストが実行され、主要な情報がハードディスク ドライブに書き込まれます。この情報は半永久的に記録されます。DPSが実行されるたびに、テストの結果がハードディスク ドライブに書き込まれます。HPのサポート窓口はこの情報を使用して問題の原因を診断します。DPSの使用手順については、Documentation CDに収録されている『トラブルシューティング ガイド』を参照してください。

耐サージ機能付連続供給電源装置

耐サージ機能が付いた連続供給電源によって、急激な電圧の変化に対処することができます。この電源装置は、データの損失やシステム ダウンを引き起こさずに2000 Vまでのサージ電圧に耐えられることが確認されています。

温度センサ機能

温度センサ機能は、ハードウェアとソフトウェアの統合により提供される機能で、コンピュータ内部の温度を監視します。温度が通常の範囲を超えると、画面上に警告メッセージが表示されるため、内部部品の故障やデータの損失が発生する前に対処することができます。

モデルにより温度センサ機能はサポートされない場合があります。

索引